From: **Larry Benson, Director**
LexisNexis Risk Solutions
1150 18th St NW Washington, DC 20036

To: **The Fraudulent Business Filing Working Group**
State of Colorado
Department of State
1700 Broadway, Suite 550
Denver, CO 80290

-Members of the Working Group,

Let me start by thanking you for allowing me to come in on October 26th, to address the Fraudulent Business Working Group. I certainly hope my presentation was useful and helpful. Upon leaving the meeting I had several thoughts that I would like to share, tied to additional information and the questions posed during the meeting.

During discussion about the use of a state-issued ID to verify the identity of a registered agent, Deputy Secretary Beall referenced the ability to use the DMV database to verify that an ID is legitimate. The missing piece in this process is verification of the ID holder at the time of submittal (e.g. Is it being submitted by the same party that is pictured on the license?). Authenticating the submitting party by requiring that a motion-detected selfie be submitted alongside a photo of the ID during the application process would solve the problem of unauthorized use by a third party. This process, which takes less than 60 seconds, would simply entail providing a picture of the ID and a selfie, leveraging automated facial recognition to assure a match; many organizations and government agencies already use a similar process for identity authentication. An added benefit is that the name, address, date of birth, and license number are automatically populated into the application which simplifies and speeds up the process. Such a process would help eliminate business identity theft on the front-end by verifying that a registered agent is who they say they are, currently resides in Colorado, and is not deceased.

The next topic for which I'd like to provide additional information is in response to Mr. Calvin's question regarding the potential impact on registration by those who

are unbanked. Assuming that the registration is being done on-line, and not in person, an unbanked individual must still fill out the business registry application and pay associated fees. If an individual is unbanked, they are unlikely to have access to a credit card to make such a payment. Therefore, their best options would be to either register in person, or buy a prepaid Visa or Mastercard to make the payment on-line. I think it is important to note that this issue would arise regardless of implementing a front-end identity verification requirement.

Overall, front-end identity authentication would be a very low friction process for the applicant and would serve the dual purpose of permitting legitimate applicants to register quickly while protecting against business identity theft before it happens. While we are currently in discussions with several Secretary of State offices around the country, the solutions that I have suggested are already standard and are being used by both government and commercial organizations. The Mississippi Secretary of State has successfully deployed our digital identity solution (a token-based consortium solution that uses device attributes, including IP address, to help verify an identity) as they were experiencing hundreds of fraudulent Russian registrations and needed to stop them. To date LexisNexis Risk Solutions leverages this same technology in all fifty states, hundreds of agencies, over 3,900 law enforcement agencies, and a multitude of federal agencies to assist with identity authentication across programs including unemployment, DMVs, SNAP, and FEMA.
I hope this helps clarify some of the discussion points. I commend members of the Working Group for working to identify solutions to this growing problem.

Thank you for your time,
Larry Benson